

# United States District Court

for the  
Western District of New York

## In the Matter of the Search of

(Briefly describe the property to be searched or identify the person by name and address.)

Information associated with email account Brettlutz2012@yahoo.com stored at premises controlled by Yahoo, Inc.

Case No. 16-M-1010

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that there is now concealed on the following person or property located in the Northern District of California (identify the person or describe the property to be searched and give its location):

Information associated with email account Brettlutz2012@yahoo.com stored at premises controlled by Yahoo, Inc., as more fully described in Attachment A.

The person or property to be searched, described above, is believed to conceal (identify the person or describe the property to be seized):

See Attachment B

The basis for search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to violations of 18 U.S.C. Sections 2252A(a)(5)(B) and 2252A(a)(2)(A).

The application is based on these facts:

- ☒ continued on the attached sheet.
- ☐ Delayed notice of \_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

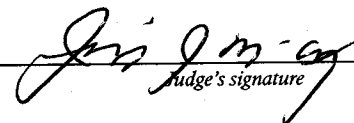
CHAD W. ARTRIP  
SPECIAL AGENT  
FEDERAL BUREAU OF INVESTIGATION

Printed name and title

Sworn to before me and signed in my presence.

Date: February 4, 2016

City and state: Buffalo, New York



Judge's signature

HONORABLE JEREMIAH J. MCCARTHY  
UNITED STATES MAGISTRATE JUDGE

Printed name and Title

**ATTACHMENT A**

**Property to Be Searched**

This warrant applies to information associated with:

Brettlutz2012@yahoo.com

for the date range: January 1, 2015 through Present, that is stored at premises owned, maintained, controlled, or operated by YAHOO!, Inc., a company headquartered at 701 First Ave, Sunnyvale, California 94089.

**ATTACHMENT B**

**Particular Things to be Seized**

**I. Information to be disclosed by YAHOO!, Inc.**

To the extent that the information described in Attachment A is within the possession, custody, or control of YAHOO!, Inc., YAHOO!, Inc. is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. The contents of all e-mails stored in the account, including copies of e-mails sent to and from the account, draft e-mails, the source and destination addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail;

b. The contents of all instant messages stored in the account, including copies of messages sent to and from the account, draft messages, the source and destination addresses associated with each message, the date and time at which a message was sent/received, and the size and length of each message;

c. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, and/or log files;

d. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;

e. All records pertaining to communications between YAHOO!, Inc. and any person regarding the account, including contacts with support services and records of actions taken.

## **II. Information to be searched for and seized by the government**

All information described above in Section I that constitutes fruits, evidence, and instrumentalities of violations of Title 18, United States Code, Section 2252A(a)(5)(B) (Possession of Child Pornography) and Title 18, United States Code, Section 2252A(a)(2)(A) (Receipt and/or Distribution of Child Pornography) associated with Yahoo! email account brettlutz2012@yahoo.com and/or others associated with and/or communicating with Yahoo! email account brettlutz2012@yahoo.com, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

a. Communications, images or videos related to the possession, solicitation or production of images depicting minors engaging in sexually explicit conduct; or

b. Evidence of the possession, receipt, production or distribution of images depicting minors engaging in sexually explicit conduct; or

c. Records relating to who created, used, or communicated with the account or identifier, including records about their identities and whereabouts.

**AFFIDAVIT**

STATE OF NEW YORK    )  
COUNTY OF ERIE        )    SS:  
CITY OF BUFFALO        )

I, **SA Chad W. Artrip**, being duly sworn, depose and say:

1. I am a Special Agent of the Federal Bureau of Investigation and entered on duty in 2007. I am currently assigned to the Buffalo Field Office, Jamestown, New York Resident Agency and work on a variety of investigative matters to include cases associated with the Violent Crimes Against Children program, which targets individuals involved in the on-line sexual exploitation of children. As part of these duties, I have become involved in the investigation of suspected violations of Title 18, United States Code, Sections 2251, 2252, 2252A, 2422, and 2423.

2. I make this affidavit in support of an application for a search warrant for information associated with a specific email account, during a specific time period, which is stored at premises owned, maintained, controlled, or operated by YAHOO!, Inc., an e-mail provider headquartered at 701 First Ave, Sunnyvale, California 94089. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require YAHOO!, Inc. to disclose to the government records and other information in its possession pertaining to the subscriber or customer associated with the accounts, including the contents of communications.

3. The statements contained in this affidavit are based on my involvement in this investigation, as well as information provided to me by other law enforcement officers involved in this investigation, and upon my training and experience. Because this affidavit is being submitted for the limited purpose of seeking a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence of violations of Title 18, United States Code, Section 2252A(a)(5)(B) (Possession of Child Pornography) and Section 2252A(a)(2)(A) (Receipt and/or Distribution of Child Pornography) exists within a specific Yahoo! email account, during a specific time period, further described in Attachment A, which is stored at premises owned, maintained, controlled, or operated by YAHOO! Inc.

4. Title 18, United States Code, Section 2252A pertains to federal child pornography laws in which computers are used as the means for producing, receiving, transmitting, and storing child pornography, in relation to the sexual exploitation of children. Child pornography is defined in Title 18, United States Code, Section 2256.

#### **I. SPECIFIC INTERNET APPLICATIONS AND WEBSITES**

5. Yahoo! is an Internet search engine that also provides users with e-mail and instant messaging/chat services that allow users to communicate via the Internet with other Internet users. In order to use the email features of Yahoo!, an individual must register with Yahoo! by establishing a unique screen name, user profile, and password. During registration or at any time after registration, an individual may add other personal

information, such as their name, address, telephone number, interests, etc., to their user profile. After registration is complete with Yahoo!, an email account will be established and made accessible for the individual with the email address [unique screen name]@yahoo.com. Once an account has been established, the individual will also have the ability to access Yahoo! Instant Message (IM). The individual's Yahoo! IM screen name will be the same as their unique screen name associated with their Yahoo! email address.

## **II. DETAILS OF THE INVESTIGATION**

6. On or about November 29, 2015, M.P. (hereinafter Complainant), had to unexpectedly travel following the death of a family member. Rather than take her fifteen year old son (hereinafter Victim 1) with her, the Complainant asked her neighbor, Brett LUTZ to stay with Victim 1 at her residence until her return. LUTZ agreed and did stay with Victim 1 at the Complainant's residence in Jamestown, New York.

7. On or about December 2, 2015, the Complainant returned to her residence. Victim 1 and a number of his friends were also at Complainant's residence. On that date, Victim 1 and his friends told the Complainant that they had located a video of LUTZ performing oral sex on Victim 1. Further, Victim 1 told the Complainant that LUTZ had likely distributed the video over the Internet.

8. Victim 1 and his friends were able to see the video because LUTZ had used a mobile device belonging to one of Victim 1's friends and left his accounts open on the referenced device.

9. After learning of the allegation, the Complainant contacted the Jamestown Police Department to file a complaint.

10. After contacting the Jamestown Police Department, the Complainant was shown what was purported to be LUTZ' email account on one of Victim 1's friend's mobile devices. The Complainant did not see a video depicting LUTZ performing oral sex on Victim 1. However, the Complainant did see several electronic file folders with pictures on top of the files folders. In your affiant's experience, pictures on top of electronic file folders are previews or "thumbnails" of what is contained within the file folder.

11. The images displayed as previews of what was contained in the electronic files contained depictions of prepubescent males engaged in lewd and/or lascivious displays of their genitals. The Complainant specifically recalled viewing an image that depicted two prepubescent males facing one another while grasping one another's genitals.

12. Although the Complainant did contact the Jamestown Police Department before viewing the referenced images, the Complainant was not instructed to view the images by the Jamestown Police Department or any other law enforcement entity.



13. The Complainant did confront LUTZ regarding the allegations that he sexually abused Victim 1 and subsequently producing a video of the abuse. LUTZ asked the Complainant not to contact law enforcement because he did not want to go to prison.

14. On December 3, 2015, at the direction of Detectives of the Jamestown Police Department, Victim 1 placed a consensually monitored telephone call to LUTZ. During the telephone call, LUTZ admitted to performing oral sex on Victim 1 and to producing a video of the act. LUTZ further admitted to distributing the video over the Internet.

15. On December 3, 2015, a preservation letter was provided to Yahoo requesting the retention of information regarding Yahoo email address brettlutz2012@yahoo.com.

16. On December 4, 2015, LUTZ was interviewed by your affiant and Detectives of the Jamestown Police Department. LUTZ was questioned regarding his use of e-mail. LUTZ stated that his email address is brettlutz2012@yahoo.com. LUTZ also advised that he has used the email address brettlutz94@yahoo.com in the past but has not used that email address in some time.

17. During the interview, LUTZ did confess to performing oral sex on Victim 1 and producing a video of the referenced sex act. LUTZ further admitted to distributing the video via social media.

18. In addition to the referenced sex act involving Victim 1, LUTZ also admitted to performing oral sex on Victim 2. According to Lutz, Victim 2 is a twelve year old male. LUTZ stated the incident involving Victim 2 occurred approximately eight months prior to the interview. LUTZ further admitted to producing a video of the sex act with Victim 2. LUTZ stated that he used Victim 1's Ipod to produce the video of the sex act with Victim 2. LUTZ further stated he distributed the video of the incident involving Victim 2 via social media.

19. During the interview, LUTZ stated that he distributed the referenced material to Tyler Callahan and Ryan Quinn. LUTZ is only friends with Callahan and Quinn on Facebook and does not know either individual personally.

20. On December 29, 2015, your affiant interviewed Lacy Wagner, step-mother of a friend of Victim 1. Wagner stated that on December 2, 2015, her step-son showed her what he purported to be LUTZ' email account. The email account was viewed on Wagner's step-son's mobile telephone. Wagner's step-son was able to view LUTZ' email account because LUTZ had provided Wagner's step-son with LUTZ' password for his email account.

21. Wagner does not recall which email service provider displayed on her step-son's mobile telephone, but does recall the name "Brett William Lutz" being displayed at the top of the screen.

22. Wagner stated she saw an array of electronic file folders contained within LUTZ' email account that had pictures displayed on top of the file folders. In your affiant's experience, images displayed on top of an electronic file folder are typically preview images of the data contained in the electronic file folder. Wagner described the images as being of prepubescent males engaging in lewd and lascivious displays of their genitals.

23. Wagner stated she recalled the names of several of the electronic file folders. The labels of the file folders include, but are not limited to, "(Victim 1's First Name)'s penis" and "(Victim 2's First Name)'s penis."

24. On December 31, 2015, a Federal Search Warrant was executed on Facebook commanding the production of the content of LUTZ', Callahan's, and Quinn's Facebook account. The material contained within the referenced accounts did contain what appears to be images of Victim 1's erect penis and chat conversations that indicate the referenced images were distributed by LUTZ to Callahan and Quinn.

25. Further, the chat conversations contained in Callahan's Facebook account indicate that LUTZ had provided Callahan with additional child pornography using an email service. An excerpt of an October 13, 2015 chat session between LUTZ and Quinn is as follows:

LUTZ: I did suck a boy that was 12 that was more mature down there and he did and idk he wouldn't cum tho

LUTZ: I have a picture of his penis I can send u

Quinn: The 12 year old?

LUTZ: yeah

LUTZ: I'll send it on ur email

Quinn: OK. How long ago u suck him

LUTZ: That was about three months ago the one night I got him naked and had a chance to put it in him but I didn't want to make him scream or moan loud bc his older brother was in the other room.

LUTZ: didroom (sic) did u get the pics

Quinn: What was his name

Quinn: And how did u no (sic) him?

LUTZ: His name is (Victim 2 First Name) and bc his older brother and I are best friends.

---

26. Quinn asked LUTZ for a picture of the individual referenced in the October 13, 2015 chat session. In reply, LUTZ sent an facial image of a young male. Jamestown Police Detectives confirmed the young male depicted in the referenced image as being Victim 2.

### **III. COMPUTERS AND CHILD PORNOGRAPHY**

27. Computers and computer technology, such as smart phones, have revolutionized the way in which individuals interested in child pornography interact with others. Child pornography formerly was produced using cameras and film (either still photography or movies). The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. There were definable costs involved with the production of pornographic images. To distribute these images on any scale required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contacts, mailings, and telephone calls.

28. The development of computers has significantly reduced the amount of resources needed to produce, communicate, distribute, share, and possess child pornography.

29. Child pornographers can now transfer photographs from a camera into a computer readable format with a device known as a scanner. With the advent of digital cameras, the images can now be captured on a digital camera and transferred directly onto a computer. A device known as a modem allows any computer to connect to another computer through the use of a telephone, cable, or wireless connection. Additionally, it is now commonplace for cellular telephones to be equipped with photo and video capabilities, which allow an individual to digitally shoot, store, send, and/or receive child pornography all

with one device. Electronic contact can be made to literally millions of computers around the world.

30. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store hundreds of thousands of images at very high resolution.

31. The Internet and its World Wide Web afford collectors of child pornography several different venues for obtaining, viewing and trading child pornography in a relatively secure and anonymous fashion.

32. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides email services as well as electronic storage of computer files in a variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer.

33. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an email as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or Internet Service Provider client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Additionally, a computer also creates logs, indices, and registries indicating when a computer was used, which user was logged on, and when data was accessed, shared, transferred, or downloaded. A forensic examiner can often recover evidence which shows that a computer contains peer to peer software, when the computer was sharing files, and even some of the files which were uploaded or downloaded. Such information may be maintained indefinitely until overwritten by other data.

34. The Internet is a worldwide computer network that connects computers and allows communications and the transfer of data and information across state and national boundaries. A user accesses the Internet from a computer network or Internet Service Provider (ISP) that connects to the Internet. The ISP assigns each user an Internet Protocol (IP) Address. Each IP address is unique. Every computer or device on the Internet is referenced by a unique IP address the same way every telephone has a unique telephone number. An IP address is a series of four numbers separated by a period, and each number is

a whole number between 0 and 255. An example of an IP address is 192.168.10.102. Each time an individual accesses the Internet, the computer from which that individual initiates access is assigned an IP address. A central authority provides each ISP a limited block of IP addresses for use by that ISP's customers or subscribers. Most ISP's employ dynamic IP addressing, that is, they allocate any unused IP address at the time of initiation of an Internet session each time a customer or subscriber accesses the Internet. A dynamic IP address is reserved by an ISP to be shared among a group of computers over a period of time. IP addresses may also be static, if an ISP assigns a user's computer a particular IP address that is used each time that computer accesses the Internet. The ISP may log the date, time and duration of the Internet session for each IP address and can identify the user of that IP address for such a session from these records, depending on the ISP's record retention policies. For mobile/cellular computer technology, such as smart phones, ISPs typically assign massive numbers of mobile/cellular devices to one IP address. This has made identifying the user of a specific mobile/cellular device extremely difficult, if not impossible, when presented with only an IP address.

35. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little to no cost. Even when such files have been deleted, they may be recoverable months or years later using readily available forensic tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive



until it is overwritten by new data. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

#### **IV. TECHNICAL BACKGROUND - EMAIL**

36. In my training and experience, I have learned that YAHOO!, Inc. provides a variety of on-line services, including electronic mail ("e-mail") access, to the general public. YAHOO!, Inc. allows subscribers to obtain e-mail accounts at the domain name yahoo.com, like the e-mail account listed in Attachment A. Subscribers obtain an account by registering with YAHOO, Inc. During the registration process, YAHOO!, Inc. asks subscribers to provide basic personal information. Accordingly, the computers of YAHOO!, Inc. are likely to contain stored electronic communications (including retrieved and un-retrieved e-mail for YAHOO!, Inc. subscribers) and information concerning subscribers and their use of YAHOO!, Inc. services, such as account access information, e-mail transaction information, and account application information.

37. In general, an e-mail that is sent to a YAHOO!, Inc. subscriber is stored in the subscriber's "mail box" on YAHOO!, Inc. servers until the subscriber deletes the e-mail. If the subscriber does not delete the message, the message can remain on YAHOO!, Inc. servers indefinitely.

38. When the subscriber sends an e-mail, it is initiated at the user's computer, transferred via the Internet to YAHOO!, Inc.'s servers, and then transmitted to its end destination. YAHOO!, Inc. often saves a copy of the e-mail sent. Unless the sender of the e-mail specifically deletes the e-mail from the YAHOO!, Inc. server, the e-mail can remain on the system indefinitely.

39. A sent or received e-mail typically includes the content of the message, source and destination addresses, the date and time at which the e-mail was sent, and the size and length of the e-mail. If an e-mail user writes a draft message but does not send it, that message may also be saved by YAHOO!, Inc. but may not include all of these categories of data.

40. A YAHOO!, Inc. subscriber can also store files, including e-mails, address books, contact or buddy lists, calendar data, pictures, and other files, on servers maintained and/or owned by YAHOO! Inc., which allows users to search for videos on the internet; Google Talk, which allows users to send instant messages and/or place online telephone calls to other internet users; and Picasa, which allows users to store and share digital images.

Further, YAHOO! has a chat application that allows users to send and receive instant messages, which may be stored on and retrieved from YAHOO!, Inc. servers.

41. Subscribers to YAHOO!, Inc. might not store emails on their home computers that may be stored in their YAHOO!, Inc. account. This is particularly true when they access their YAHOO!, Inc. account through the web, or if they do not wish to maintain particular e-mails or files in their residence.

42. In general, e-mail providers like YAHOO!, Inc. ask each of their subscribers to provide certain personal identifying information when registering for an e-mail account. This information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative e-mail addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number).

43. E-mail providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via YAHOO!, Inc.'s website), and other log files that reflect usage of the account. In addition, e-mail providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular

logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the e-mail account.

44. In some cases, e-mail account users will communicate directly with an e-mail service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. E-mail providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications.

45. In my training and experience, evidence of who was using an e-mail account may be found in address books, contact or buddy lists, e-mail in the account, and attachments to e-mails, including pictures and files.


#### **V. INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED**

46. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require YAHOO!, Inc. to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. Upon receipt


of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

## VI. CONCLUSION

47. Based upon the above information, I believe probable cause exists that there have been violations of Title 18, United States Code, Section 2252A(a)(5)(B) (Possession of Child Pornography) and Title 18, United States Code, Section 2252A(a)(2)(A) (Receipt and/or Distribution of Child Pornography), and that there is probable cause to believe that within a specific Yahoo! email account, further described in Attachment A, that is stored at premises owned, maintained, controlled, or operated by YAHOO! Inc., there are items described in Attachment B, which are evidence of and fruits and instrumentalities of such violations. Accordingly, I respectfully request that this Court issue a search warrant for the Yahoo! email account, further described in Attachment A, authorizing the search of the aforementioned account for the items described in Attachment B. Finally, I respectfully request that this Affidavit be sealed until further order of the Court, as this is an ongoing investigation, and because, prior to the filing of any criminal charges, it would be unduly prejudicial to the subject of this investigation to disclose his identity publicly.

  
CHAD W. ARTRIP  
Special Agent  
Federal Bureau of Investigation

Sworn to before me this 4TH  
day of February, 2016.

  
JEREMIAH J. MCCARTHY  
United States Magistrate Judge

**ATTACHMENT A**

**Property to Be Searched**

This warrant applies to information associated with:

Brettlutz2012@yahoo.com

for the date range: January 1, 2015 through Present, that is stored at premises owned, maintained, controlled, or operated by YAHOO!, Inc., a company headquartered at 701 First Ave, Sunnyvale, California 94089.

**ATTACHMENT B**

**Particular Things to be Seized**

**I. Information to be disclosed by YAHOO!, Inc.**

To the extent that the information described in Attachment A is within the possession, custody, or control of YAHOO!, Inc., YAHOO!, Inc. is required to disclose the following information to the government for each account or identifier listed in Attachment A:

- a. The contents of all e-mails stored in the account, including copies of e-mails sent to and from the account, draft e-mails, the source and destination addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail;
- b. The contents of all instant messages stored in the account, including copies of messages sent to and from the account, draft messages, the source and destination addresses associated with each message, the date and time at which a message was sent/received, and the size and length of each message;
- c. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, and/or log files;

d. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;

e. All records pertaining to communications between YAHOO!, Inc. and any person regarding the account, including contacts with support services and records of actions taken.

**II. Information to be searched for and seized by the government**

All information described above in Section I that constitutes fruits, evidence, and instrumentalities of violations of Title 18, United States Code, Section 2252A(a)(5)(B) (Possession of Child Pornography) and Title 18, United States Code, Section 2252A(a)(2)(A) (Receipt and/or Distribution of Child Pornography) associated with Yahoo! email account brettlutz2012@yahoo.com and/or others associated with and/or communicating with Yahoo! email account brettlutz2012@yahoo.com, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

a. Communications, images or videos related to the possession, solicitation or production of images depicting minors engaging in sexually explicit conduct; or

b. Evidence of the possession, receipt, production or distribution of images depicting minors engaging in sexually explicit conduct; or

c. Records relating to who created, used, or communicated with the account or identifier, including records about their identities and whereabouts.